IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

DEFENDANT ATTORNEY GENERAL MAURA HEALEY'S BRIEF ON TEXTUAL INTERPRETATION OF THE DATA ACCESS LAW

MAURA HEALEY
ATTORNEY GENERAL

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Christine Fimognari, BBO No. 703410
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, Mass. 02108
(617) 963-2178
Robert.Toone@mass.gov

Dated: October 14, 2022

CONTENTS

Defendant Attorney General Maura Healey respectfully submits this brief on textual interpretation of the Data Access Law, as directed by the Court on September 22, 2022. *See* ECF No. 286.

The facial, pre-enforcement nature of the preemption claims brought by the plaintiff Alliance for Automotive Innovation ("Alliance") determines both the Alliance's burden of proof and the manner in which the Data Access Law must be interpreted in this proceeding. Even if the Alliance had a private right of action to challenge the law as preempted by either the Federal Motor Vehicle Safety Act ("MVSA") or Clean Air Act ("CAA"), *but see* ECF No. 232 (Attorney General's Proposed Revised Substitute Findings of Fact and Conclusions of Law) at CL ¶¶ 11-28 – or associational standing to assert those claims on behalf of its members, even though the evidence has shown that OEMs can and have taken different approaches to complying with the law and some are already in compliance, *see id.* at CL ¶¶ 1-10; ECF No. 263 at 15-19 – to prevail on the merits of those claims the Alliance must prove that "no set of circumstances" exists under which any OEM could comply with the MVSA or CAA, on the one hand, and the Data Access Law on the other. *NCTA – The Internet & TV Ass'n v. Frey*, 7 F.4th 1, 17 (1st Cir. 2021). The "current design" of the OEMs' vehicles is irrelevant; all that matters is whether there is any possible future implementation of the Data Access Law that would not violate federal law. *See CDK Glob. LLC v. Brnovich*, 16 F.4th 1266, 1275 (9th Cir. 2021).

The Alliance has failed to meet that high burden. First, there is no provision in the MVSA or CAA, or any regulation promulgated thereunder, that conflicts with the Data Access Law on its face. No federal law or regulation addresses the cybersecurity of motor vehicles or access to motor vehicle diagnostic data. The decision of the NHTSA and EPA not to regulate these issues "is fully consistent with an intent to preserve state regulatory authority pending the

adoption of specific federal standards," *Sprietsma v. Mercury Marine*, 537 U.S. 51, 65 (2002), and the Alliance cannot rely on non-binding agency guidance or policy about cybersecurity or difficulty of implementation as support for its claims, *Kansas v. Garcia*, 140 S. Ct. 791, 801 (2020) (citation omitted).[1] Even now, the Alliance tellingly frames its objections to the Data Access Law in terms of the supposed "loss of cybersecurity protections" and "cybersecurity risks" – not as a conflict with any specific federal statute or regulation. ECF No. 290 at 3-10, 12-15.

Furthermore, even if there were a federal law in potential conflict, a facial preemption claim like this one presumes that Massachusetts courts will interpret the Data Access Law to avoid such a conflict. Because the Alliance brought this lawsuit "against a sovereign State" to challenge the law "before [it] has gone into effect," to the extent there is any uncertainty about "what the law means," it would be inappropriate "without the benefit of a definitive interpretation from the state courts" to assume that those courts will construe the law "in a way that creates a conflict with federal law." *Arizona v. United States*, 567 U.S. 387, 415 (2012); *see also Wash. State Grange v. Wash. State Rep. Party*, 552 U.S. 442, 449-50 (2008) ("[W]e must be careful not to go beyond the statute's facial requirements and speculate about 'hypothetical' or 'imaginary' cases," because the "State has had no opportunity to implement" the law, "and its courts have had no occasion to construe the law in the context of actual disputes . . . , or to

[1] The United States has declined to claim preemption in this case. *See* ECF No. 202 at 1, 10. Rather, the National Highway Traffic Safety Administration (NHTSA) has repeatedly urged the automotive industry to "provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner." ECF No. 232 at CL ¶ 81 (discussing 2016 and 2020 NHTSA cybersecurity guidance); *see also* National Highway Traffic Safety Administration, *Cybersecurity Best Practices for the Safety of Modern Vehicles* 13 (2022) (same), available at https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf.

accord the law a limiting construction to avoid constitutional questions.") (citations omitted). It is well established that Massachusetts courts in fact do construe state laws to avoid federal preemption. *Wright's Case*, 486 Mass. 98, 108 (2020) (citing *Ajemian v. Yahoo!, Inc.*, 478 Mass. 169, 184 (2017)).

As discussed below, the Attorney General and Alliance agree on the meaning of certain key terms in the Data Access Law, including the terms "motor vehicle," "standardized," "entity unaffiliated with a manufacturer," "telematics system," "interoperable," and "platform." They disagree on the meaning of other terms, and those disagreements reflect the fundamental differences in how the parties have approached this litigation. The Attorney General has proffered interpretations based on the plain text of the Data Access Law, the law's purpose and overall structure, and well-established meanings of technical terms of art. The Alliance, by contrast, has interpreted terms in their "broadest form" possible, all in an effort to make the law seem focused on data unrelated to the diagnosis, repair, and maintenance of vehicles; incompatible with security and safety controls; and impossible to implement. None of that is true, as the Alliance's own experts ultimately conceded during the hot tub discussion at trial. Because they have no merit, this Court should now reject the Alliance's preemption claims and allow the Data Access Law to take effect.

I. THE PARTIES AGREE ON THE MEANING OF CERTAIN STATUTORY TERMS.

The Parties' Joint Submission Regarding Textual Interpretations of Data Access Law, ECF No. 290, shows that they agree on the meanings of several key provisions in the law.

The parties agree that the term "motor vehicle," which is used in both Section 2 and 3 of the Data Access Law, means any "vehicle, originally manufactured for distribution and sale in the United States, driven or drawn by mechanical power and manufactured primarily for use on

public streets, roads and highways," with certain exceptions set forth in Mass. G.L. c. 93K, § 1. ECF No. 290 at 2-3. They further agree that this definition includes cars powered by internal combustion engines and electric cars. *Id.* at 3. The Alliance agrees on this definition notwithstanding its expert Bryson Bort's testimony at trial that he believed "motor vehicle" was defined as having "an internal combustion engine" and that electric vehicles are not subject to the law. Tr. III:99.

The parties generally agree on the meaning of the terms "standardized" and "standardized across all makes and models sold in the Commonwealth." ECF No. 290 at 4-5. The term "standardized" means following a common and well documented method to perform a necessary action such that there is a common, agreed upon way of communicating. *Id.* The term "standardized across all makes and models sold in the Commonwealth" in Section 2 of the Data Access Law is not limited to the makes and models of a particular manufacturer, whereas the standardization requirement in Section 3 is so limited. *Id.*

The parties also agree that the term "entity unaffiliated with a manufacturer," as used in Section 2, means an entity that does not have a formal corporate affiliation with an OEM or is subject to an OEM's direct or indirect control. ECF No. 290 at 7-8. The evidence at trial established that "an entity unaffiliated with a manufacturer" can be created without compromising the security or integrity of vehicle networks or requiring the removal of access controls. ECF No. 232 at FF ¶¶ 178-79; . Such an unaffiliated entity can be readily created, but the OEMs have refused to work with others in the auto industry to do so. ECF No. 232 at FF ¶¶ 46-49, 192-96; ECF No.191 (Lowe Aff.) ¶¶ 68-74, 82, 88-89; Tr. II:88-89.

With respect to terms used in Section 3, the parties agree that the term "telematics system" means any "any system in a motor vehicle that collects information generated by the

operation of the vehicle and transmits such information . . . utilizing wireless communications to a remote receiving point where it is stored." ECF No. 290 at 9. They agree that the term "interoperable" means a standard way to connect and communicate with the vehicle; an interoperable device is one that can be used regardless of the manufacturer. *Id.* at 9-11. The parties agree that the term "standardized" in Section 3 means following a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating. *Id.* at 11. And the parties agree that the term "platform" means the vehicle architecture and associated software and features. *Id.* at 12-13.

II. WITH OTHER TERMS, THE ALLIANCE HAS PROPOSED OVERBROAD INTERPRETATIONS IN AN ATTEMPT TO CREATE A CONFLICT WITH FEDERAL LAW.

On the meaning of other terms in the Data Access Law, the parties disagree. As discussed in Section III, *infra*, the interpretations set forth by the Attorney General are reasonable, supported by expert testimony, and consistent with well-established principles of statutory construction. Because the Data Access Law assigns to the Attorney General responsibility for the enforcement and public dissemination of information about the law, *see* Mass. G.L. c. 93K, §§ 2(g) (notice requirement) & 6 (enforcement), her interpretations are also entitled to "substantial deference." *See Goldberg v. Bd. of Health of Granby*, 444 Mass. 627, 633 (2005) (citation omitted). In evaluating a facial challenge of the type asserted by the Alliance, courts are "required" to "consider any limiting construction that a state court or enforcement agency has proffered," *Nat'l Org. for Marriage v. McKee*, 649 F.3d 34, 66 (1st Cir. 2011) (citation omitted), and the Commonwealth's proffered interpretation is entitled to "great weight," *McGuire v. Reilly*, 386 F.3d 45, 55, 64 (1st Cir. 2004); *accord March v. Mills*, 867 F.3d 46, 67 (1st Cir. 2017) (finding "no reason not to accept [the Maine Attorney General's] perfectly

sensible representation about how the disruptive-intent requirement [of challenged state statute] operates").

By contrast, the Alliance's contested definitions reflect its trial strategy of interpreting key provisions in the Data Access Law extremely broadly and then arguing that the law, so interpreted, conflicts with federal law. For example, Mark Chernoby, Chief Technical Compliance Officer for FCA, testified that where he viewed a term in the Data Access Law as vague or ambiguous, he had "to interpret it in the broadest form to make sure our vehicles comply." Tr. I:126. That blunderbuss approach to statutory interpretation is entitled to no deference and, indeed, contradicts the Supreme Court's admonition that state laws must be "read to avoid [preemption] concerns" whenever possible. *Arizona*, 567 U.S. at 413-15.

Importantly, when confronted at trial with the more reasonable interpretations advanced by the Attorney General's experts, the Alliance's experts conceded that the Data Access Law could be readily implemented without violating federal law. For example, prior to the hot tub, the Alliance's expert Bort testified that he interpreted the term "mechanical data" (as used in Section 3) to encompass, among other things, (i) all ECUs' firmware, (ii) all manner of internal messages that concerned the vehicle's operation, and (iii) diagnostic functions that are reserved for engineering and manufacturing. Tr. I:187-88.[2] At the hot tub, however, the Attorney General's expert Craig Smith testified that he understood "mechanical data" to require not access to all vehicle data, but rather just a "level playing field" with respect to data used by automotive dealerships to diagnose, maintain, and repair vehicles. Tr. III:55-56. Bort then conceded that,

[2] Similarly, Kevin Baltes, Director of Product Cyber Security at GM, testified that, under "my interpretation of section 2," the Data Access Law "requires broad access to data that is not necessary for vehicle diagnosis, maintenance and repair," Tr. I:109-10, and Kevin Tierney, VP Global Cybersecurity at GM, testified that, under his interpretation, the Data Access Law requires access "to a nearly limitless volume of vehicle data," Tr. I:54.

under that more reasonable interpretation of "mechanical data" (which is consistent with the text, structure, and purpose of the law, *see* Section III.B.3, *infra*), "that's a different scope, and I wouldn't have an issue with that," Tr. III:79. The Alliance's other expert Daniel Garrie agreed that, when the law is interpreted in a more pragmatic fashion, "[i]t seems a lot more feasible." Tr. III:58.

Similarly, Bort initially testified that he interpreted the term "open access" in Section 3 to mean that "anyone can have access to the insides of a vehicle." Tr. I:189. His opinion of the risks posed by the Data Access Law flowed from his view that the required level of access includes "the potential to reprogram and do firmware and software development." Tr. III:68-69.[3] At the hot tub, however, Bort conceded that, under the more pragmatic interpretation advanced by the Attorney General's experts, *see* Section III.B.3, *infra*, their solutions were "not far-fetched," Tr. III:70-71, and would involve only "a minor level of doing that risk assessment and potential rearchitecture," which he "wouldn't anticipate . . . being an exponentially burdensome piece," Tr. III:75.

The hot tub conversation thus proved that the Alliance's claims cannot survive reasonable interpretations of the Data Access Law. Nevertheless, now – 16 months after trial – the Alliance has reasserted its original, overbroad definitions, in the hope that the Court will adopt them and find some conflict with some unidentified provision of federal law. Its approach disregards both the trial record and the applicable law on federal preemption.

[3] Similarly, Chernoby testified that his "interpretation" of the "open access" requirement was that FCA would have to remove or disable access controls – "an automaker would have no ability to put any protection and/or roadblock in to access those systems." Tr. I:123-24, 126. Tierney testified that he believed "the law requires access to every electronic network component of the vehicle encompassing components far beyond anything even remotely related to vehicle diagnosis, repair or maintenance." Tr. I:55. Baltes testified that the Data Access Law "requires unfettered bidirectional unauthorized access to GM's vehicles and vehicle networks." Tr. I:110.

III. THE TEXTUAL INTERPRETATIONS SET FORTH BY THE ATTORNEY GENERAL ARE REASONABLE, SUPPORTED BY EXPERT TESTIMONY, AND SHOULD BE ADOPTED FOR PURPOSES OF THIS FACIAL LAWSUIT.

A. Disputed terms in Section 2

1. "Access to vehicle on-board diagnostic systems" and "access to vehicle networks and their on-board diagnostic systems"

The Attorney General interprets the phrase "access to vehicle networks and their onboard diagnostic systems" in Section 2 to refer only to access for obtaining data related to the purposes of diagnosis, repair, and maintenance. ECF No. 290 at 4; Tr. Ex. 30 at 3. By contrast, the Alliance contends that the Attorney General's definition is only partially correct, and that the definition extends beyond that to encompass open-ended access to send and obtain data from "all of the electronic networks of the vehicle" and "a vehicle's internal computer system" for any purpose whatsoever. ECF No. 290 at 3.

The Alliance's interpretation would create inconsistency with other parts of the statute. In interpreting statutes, courts look to the overall statutory scheme so as to produce an internal consistency within the statute and construe statutory amendments with preexisting statutory language so as to construe the statute as a consistent and harmonious whole. *Food and Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000). Here, Mass. G.L. c. 93K, § 2(d)(1) governs access to "onboard diagnostic and repair information system[s]," and the amendment to that provision in Section 2 of the 2020 Right to Repair Law also concerns access to vehicle onboard diagnostic systems. Interpreting Section 2 to establish requirements for access to "vehicle networks" in addition to and separate from access to diagnostic and repair information systems would not result in a consistent and harmonious construction of the statute as amended.

Moreover, the trial testimony of Aaron Lowe, a proponent and drafter of the initiative petition, supports the Attorney General's more limited and pragmatic interpretation. Lowe testified that "[t]he intention was just to get the information necessary to repair the car" and that the term "vehicle networks" was included in an effort to include electric vehicles, which "don't have onboard diagnostic systems," in the law's coverage. Tr. II:65-67.

Additionally, the Alliance's proffered interpretation ignores the overall statutory scheme, which is limited to providing data for diagnosis, maintenance, and repair. It is a "fundamental canon of statutory construction" that "the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *W. Virginia v. Envtl. Protec. Agency*, 142 S. Ct. 2587, 2607 (2022) (quoting *Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989)); *accord Richardson v. UPS Store, Inc.*, 486 Mass. 126, 130-31 (2020) ("The canon of noscitur a sociis counsels that terms must be read within the context of the statute in which they appear."). The Data Access Law is focused on access for purposes of diagnosis, repair, and maintenance, and the voters enacted this law in order to ensure that, "as technology advances, drivers can continue to get their cars repaired where they want." Tr. Ex. 509 at 5 (Question 1 proponents' statement in official "Information for Voters" publication). In fact, the law expressly provides that "[n]othing in this chapter shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information provided by a manufacturer to a dealer or by a dealer to a manufacturer pursuant to the terms of a franchise agreement." G.L. c. 93K, § 5. This provision reinforces that "access to vehicle networks and their on-board diagnostic systems" is limited to access for obtaining data related to the purposes of diagnosis, repair, and maintenance.

2. "Authorization" and "authorization system"

The Attorney General interprets the term "authorization" in Section 2 to mean an actor's role or what it is and is not permitted to do on a system. ECF No. 290 at 6-7; ECF No. 232 at FF ¶ 59. Authorization is distinct from authentication, which refers to the confirmation of the identity of an individual, user, or other actor. ECF No. 290 at 6; ECF No. 232 at FF ¶ 59; ECF No. 192 (Smith Aff.) ¶¶ 181-83; ECF No. 200 (Bort. Aff.) ¶ 53; Tr. I:249. By contrast, the Alliance agrees that the term "authorization" encompasses an actor's role or what it is and is not permitted to do on a system, but disagrees that authorization is distinct from authentication and contends that "the effect of the 'authorization' language is to exclude OEMs from any authorization or authentication process for access to on-board diagnostic systems and vehicle networks." ECF No. 290 at 6.

Where a statute uses a "term of art" with an established industry meaning, a court should "assume" that the Legislature – or, in the case of a ballot initiative, the voters – "intended it to have its established [technical] meaning," absent any contrary indication. *McDermott Int'l, Inc. v. Wilander*, 498 U.S. 337, 342 (1991); *see also La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 357 (1986) (noting "the rule of construction that technical terms of art should be interpreted by reference to the trade or industry to which they apply"); *Van Buren v. United States*, 141 S. Ct. 1648, 1657 (2021) (courts must "take note of terms that carry technical meaning[s]," including "when interpreting a statute about computers"). Here, the expert evidence at trial established that the term "authorization" is distinct from "authentication" and OEMs can comply with Section 2 while maintaining authentication safeguards. ECF No. 232 at FF ¶ 59, CL ¶¶ 45-48; ECF No. 192 (Smith Aff.) ¶¶ 181-83. The evidence at trial established that the term "authorization" refers to an actor's role or what the actor is and is not permitted to do on a system, while

"authentication" represents confirmation of the identity of an individual, a company, or other actor. ECF No. 232 at CL ¶¶ 45-46; ECF No. 192 (Smith Aff.) ¶¶ 181-83; ECF No. 200 (Bort Aff.) ¶ 53; Tr. I:249.

The Alliance's position that authorization and authentication cannot be separate processes, ECF No. 290 at 6, ignores the ample trial evidence that explained distinct authentication and authorization methods, each of which can be implemented separately. *See, e.g.*, ECF No. 192 (Smith Aff.) ¶ 183; Tr. II:213 ("you can separate out the authorization and the authentication"), 219 ("while you have one step of authorization and authentication, you can actually break out the roles and the capabilities").

3. "Directly or indirectly"

The Attorney General interprets the term "directly or indirectly" in Section 2 to mean that the OEM may not require any authorization by the manufacturer itself or a third party controlled by or affiliated with the manufacturer. ECF No. 290 at 7. By contrast, the Alliance interprets the term to mean "that the OEM may not impose the requisite authorization either by itself or through some third party." *Id.*

The Alliance's definition is overbroad, imprecise, and inconsistent with the rest of the statutory text. *See Brown & Williamson*, 529 U.S. at 133. The term "directly or indirectly" must be read in conjunction with the rest of Section 2, which specifies that OEMs can impose authorization directly or indirectly if the authorization system "is administered by an entity unaffiliated with the manufacturer." Because an unaffiliated entity is a "third party" through which an OEM can require authorization, the Alliance's proffered interpretation is inconsistent with the full text of Section 2. Accordingly, OEMs can insist on the cybersecurity protection of authorization so long as they are not the ones operating the authorization system, but rather use

some unaffiliated company or organization to run the authorization system. ECF No. 232 at FF ¶¶ 175-79, 192-96.

B. Disputed terms in Section 3

1. "Open access"

The Attorney General interprets the term "open access" in Section 3 to mean having a non-gated way to gain access to the data and capabilities. ECF No. 290 at 12; ECF No. 232 at CL ¶ 54; ECF No. 192 (Smith Aff.) ¶ 115; Tr. Ex. 30 at 7. Open access requires the platform and the mechanical data it communicates to be freely accessible to the owner, without the OEM acting as a gatekeeper. ECF No. 232 at FF ¶ 54; ECF No. 192 ¶ 117. An open access platform provides a common method for any company to participate in diagnosis, maintenance, and repairs. ECF No. 192 ¶ 116. An open access platform can still use security controls to ensure the safety and privacy of the consumer. *Id.* As expert Smith explained, the requirement that the platform be "open access" "does not mean that it could not have safety and security controls." ECF No. 192 ¶ 197.

By contrast, the Alliance interprets "open access" to mean that "the relevant device or technology . . . can be accessed without restriction." ECF No. 290 at 12. That interpretation disregards the rule that "the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *W. Virginia v. EPA*, 142 S. Ct. at 2607. Section 3 identifies several restrictions on access that can, and indeed must, exist on the open-access platform. Specifically, it provides that the "open access platform" "shall be capable of *securely* communicating all mechanical data emanating directly from the motor vehicle" and "upon the *authorization of the vehicle owner*, all mechanical data shall be directly accessible by an independent repair facility or class 1 dealer . . . *limited to the time to complete the repair or for a*

period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing, and repairing the motor vehicle" (emphasis added).

The Alliance's contention that "open access" means the platform "can be accessed without restriction," ECF No. 290 at 12, ignores the restrictions on access that are required by the text of the Data Access Law itself: secure communication of mechanical data, authorization of the vehicle owner for access by an independent repair facility or class 1 dealer, and time-limited access. Because "the words of a statute must be read in their context and with a view to their place in the overall statutory scheme," *W. Virginia*, 142 S. Ct. at 2607, the term "open access" should not be interpreted to mean a method of access that is freely accessible to actors other than the vehicle's owner. ECF No. 232 at FF ¶ 54. The Alliance's strategic overreading of this statutory term ignores the related textual requirements in Section 3; its definition is plausible only if those textual requirements are read out of the statute.

2. "Securely communicating"

The Attorney General interprets the term "securely communicating" in Section 3 to mean communication in a way that authenticates the identities of the recipient and the sender, where the communication is not made known to parties other than the recipient and the sender and the integrity of the communication is not compromised. ECF No. 290 at 13; Tr. Ex. 29 at 10; ECF No. 232 at FF ¶ 74, CL ¶ 57. For its part, the Alliance defines the term to mean "transmitting data privately, without unpermitted viewing of the content of that transmission." ECF No. 290 at 13. That definition is consistent with the portion of the Attorney General's definition that "the communication is not made known to parties other than the recipient and the sender and the integrity of the communication is not compromised." *Id.* The Alliance does not, however, appear to agree that the term "securely communicating" and the process of "transmitting data

privately" encompass "communication in a way that authenticates the identities of the recipient and the sender."

The Alliance's interpretation seems to be based on its conflated understanding of "authentication" and "authorization." *See* ECF No. 290 at 6. But it defies logic for the Alliance to contend that the cybersecurity measures expressly *required* by the text of Section 3 should be interpreted so narrowly that they lose their cybersecurity value. The Alliance agrees that "authentication" refers to the "confirmation of the identity of an individual, user, or other actor." *Id.* Confirming the identity of the respective recipient and sender to make sure that only the appropriate parties receive the data is a logical component of "transmitting data privately." Certainly, there is no basis in the text of the statute to support the Alliance's position that "securely communicating" data does not include authentication. Statutory language must not be construed so as to produce an absurd result or one "manifestly at odds with the statute's intended effect." *Arnold v. United Parcel Service, Inc.*, 136 F.3d 854, 858 (1st Cir. 1998) (quoting *Parisi by Cooney v. Chater*, 69 F.3d 614, 617 (1st Cir. 1995)). Interpreting the term "securely communicating" to exclude authentication would produce an absurd result, in which the communication of data must be kept private between a sender and recipient, but the technique used to confirm the identity of the sender and recipient cannot be used.

Moreover, the Attorney General's interpretation of this technical term is supported by unrebutted expert evidence. At trial, expert Smith explained that an "important piece of wireless communications is to ensure transmitted data is protected from eavesdroppers" and "[a] secure wireless system will typically deploy . . . signing[, which is a form of authentication] to combat [eavesdropping, or 'man-in the-middle'] attacks." ECF No. 192 (Smith Aff.) ¶ 189. By contending that "securely communicating" data does not mean authenticating the identities of the

recipient and the sender, the Alliance opts to interpret this term in a way that conflicts with the expert evidence and ignores the cybersecurity protections required by Section 3 itself.

3. "Mechanical data"

The Attorney General and Alliance agree that the term "mechanical data," as used in Section 3, is defined by the Data Access Law to mean "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle," Mass. G.L. c. 93K, § 1, but they differ as to what that definition means. ECF No. 290 at 13. The Attorney General understands "mechanical data" to include the vehicle's pre-defined diagnostic functions and any data generated, stored, or transmitted by the vehicle and used for vehicle diagnostics, maintenance, or repair, but *not* data *unrelated* to diagnostics, maintenance, or repair. ECF No. 232 at CL ¶¶ 38-40. By contrast, the Alliance contends that because of the definition's use of the phrase "otherwise related to," "'mechanical data' is not limited to diagnosis, maintenance, and repair data, but actually encompasses *any* vehicle data that could have some bearing on diagnosis, maintenance, or repair issues." ECF No. 290 at 13.

The Alliance's position ignores the plain language of the Data Access Law as well as the larger statutory context and purpose. It is well established that "'a statute must be interpreted according to the intent of the Legislature ascertained from all its words construed by the ordinary and approved usage of the language, considered in connection with the cause of its enactment, the mischief or imperfection to be remedied and the main object to be accomplished, to the end that the purpose of its framers may be effectuated.'" *DiMasi v. State Bd. of Retirement*, 474 Mass. 194, 199 (2016) (quoting *Retirement Bd. of Somerville v. Buonomo*, 467 Mass. 662, 668 (2014)). A standard definition of "relate to" means "to connect (something) with (something

else)," *see, e.g.*, "Relate to," *Merriam Webster*, available at https://www.merriam-webster.com/dictionary/relate%20to, yet the Alliance's definition of "otherwise related to" would encompass vehicle data that is completely unconnected with the diagnosis, repair, and maintenance purpose of the statute.

Moreover, limiting the definition of "mechanical data" to data about diagnostics, maintenance, or repair is consistent with the other provisions of chapter 93K, which make clear that the law does not require independent repair shops to receive access to non-diagnostic and repair information. *See* ECF No. 232 at CL ¶ 40; Mass. G.L. c. 93K, § 5 ("Nothing in this chapter shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information provided by a manufacturer to a dealer or by a dealer to a manufacturer pursuant to the terms of a franchise agreement."). The Alliance's overbroad interpretation of the phrase "otherwise related to" conflicts with the explicit instruction in G.L. c. 93K, § 5 as to how the law must be construed, whereas the Attorney General's definition conforms to that instruction as well as the overarching purpose of the law.

4. "Directly accessible"

The Attorney General interprets the term "directly accessible" in Section 3 to mean that the consumer will not need to go through the OEM to perform diagnosis, maintenance, and repairs. ECF No. 290 at 14; ECF No. 232 at FF ¶ 70, CL ¶ 55; ECF No. 192 (Smith Aff.) ¶ 118. By contrast, the Alliance interprets "directly accessible" to mean "that the user (*e.g.*, the owner or repair shop) can directly connect to the platform without having to go through any intermediary, including the OEM." ECF No. 290 at 14.

The Alliance's interpretation is overly broad and would require reading out other portions of the Data Access Law. For example, it ignores the textual requirement that the platform "shall be capable of securely communicating" mechanical data. Part of "securely communicating" data is verifying the identities of the sender and recipient of the data through some manner of authentication. *See* Section III.B.2, *supra*. Read in context, "directly accessible" means that the consumer will only need to confirm that they are the ones intending to perform the diagnostics, maintenance, or repair. ECF No. 232 at FF ¶ 70; ECF No. 192 (Smith Aff.) ¶ 118.

The Alliance's definition of "directly accessible" also ignores the plain text of Section 3 by conflating the access requirements for the owner of a vehicle and a repair shop. *See* ECF No. 290 at 14 (defining term to mean that "the user (*e.g.*, the owner or repair shop) can directly connect to the platform without having to go through any intermediary, including the OEM"). But Section 3 provides different access requirements for vehicle owners and independent repair shops. In relevant part, Section 3 provides: "Such platform shall be *directly accessible by the owner of the vehicle* through a mobile-based application and, *upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility or a class 1 dealer* licensed pursuant to section 58 of chapter 140 limited to the time to complete the repair of for a period of time agreed to by the vehicle owner for purposes of maintaining, diagnosing, and repairing the motor vehicle" (emphasis added). Because this text provides that mechanical data shall only be "directly accessible" to repair shops "upon authorization of the vehicle owner," it clearly requires that repair shops can only access the mechanical data after being authorized by the vehicle owner. Thus, the term "directly accessible" cannot mean, as the Alliance argues, "directly connect[ing] to the platform without having to go through any intermediary," because that definition would conflict with the textual requirement that

authorization, administered by some intermediary, must occur before the data is directly accessible by repair shops.

Again, the Alliance posits the broadest possible interpretation of this term without considering the context in which the term is used, resulting in a definition that ignores or directly conflicts with Section 3's other textual requirements.

5. "Ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair"

The Attorney General interprets the term "ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair" in Section 3 to mean the ability to write diagnostic data to vehicle ECUs, and to transmit packets to the ECU, if necessary for the maintenance, diagnosis, or repair of a vehicle. ECF No. 290 at 15; Tr. Ex. 30 at 7; ECF No. 232 at FF ¶ 73, CL ¶ 56. By contrast, the Alliance contends that the term "refers to the user's ability to write data to any vehicle component when such writing is necessary for maintenance, diagnostic, or repair purposes." ECF No. 290 at 15.

The Alliance's interpretation of this term is overly broad, because it requires the ability to "write data to any vehicle component." *Id.* The "ability to send commands" to in-vehicle components if necessary for maintenance, diagnostics, or repair is much more limited than "writing data to any vehicle component." Tr. III:68-69 (Bort explaining that it is "a completely different ball of wax . . . on the potential risk to the vehicle" if the scope of access required by the law includes "the potential to reprogram and do firmware and software development," as opposed to being limited to sending read and write functions to ECUS limited to purposes of diagnostics, maintenance, and repair, and that if the required scope of access is reading and writing to ECUs, "[he's] good,"), 79 (same); Tr. III:84-85 (Romansky testifying that, under his understanding of the scope of access required by the law, third parties "wouldn't be able to write

their own code, . . . they wouldn't have full access to all the proprietary design details of the vehicle; they would just have a package, a binary file delivered from the OEM that they could then transmit to the vehicle and say, oh, this ECU needs an update, here it is . . . .").

Consistent with its strategy of interpreting the law in the broadest possible way, the Alliance overlooks that the "ability to send commands to in-vehicle components" is expressly limited to the purposes of maintenance, diagnostics, and repair. As the expert trial evidence established, only certain types of in-vehicle components would need to be accessed, and only certain types of command functions would need to be performed, to achieve these limited purposes. ECF No. 232 at FF ¶ 73; ECF No. 192 (Smith Aff.) ¶ 119; Tr. III:68-69, 79, 84-85; Deposition of Kevin Baltes (Apr. 15, 2021) at 136-42 (many of the commands necessary for maintenance, diagnostics, and repair are predefined in the software of the vehicle's ECUs when the vehicle is built). Moreover, these diagnostic functions may be made subject to rationality checks, which "ensure[] that before the diagnostic [command] is executed that the vehicle is in a safe condition to do so." ECF No. 192 ¶¶ 56-57 (quoting Baltes Deposition at 154); *see* Tr. II:83 (Lowe testifying that, under his understanding of the law, it does not prohibit manufacturers from continuing to limit write access to protect the safety of the car and the passengers). Accordingly, the "ability to send commands to in-vehicle components" can be given in a way that preserves security and enables independent shops and vehicle owners to make necessary repairs. Tr. Ex. 30 at 7; ECF No. 192 ¶¶ 119, 133-36, 142, 173.

CONCLUSION

The preemption claims of the plaintiff Alliance for Automotive Innovation fail as a matter of law, and the evidence submitted at and after trial has confirmed that OEMs can comply with the Data Access Law without violating the MVSA or the CAA. Accordingly, the Alliance's request for injunctive and declaratory relief should be denied, and judgment should enter in favor of the Attorney General.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL,

By her attorneys,

October 14, 2022

/s/ Robert E. Toone

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Christine Fimognari, BBO No. 703410
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, Mass. 02108
(617) 963-2178
robert.toone@mass.gov

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the CM/ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on October 14, 2022.

Robert E. Toone
Robert E. Toone